ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки

Методи ідентифікації трафіка корпоративної комп'ютерної мережі

Кваліфікаційна робота

Виконав:
ст. гр. КСМзм-21-1
Радьков Д.В.

Керівник:
доц. Лебедєв О.Г.

Мета та завдання кваліфікаційної роботи

Метою кваліфікаційної роботи є аналіз ефективних та швидкодіючих алгоритмів ідентифікації, методів та технологій передачі трафіку за рахунок підвищення якості кластеризації та класифікації трафіку.

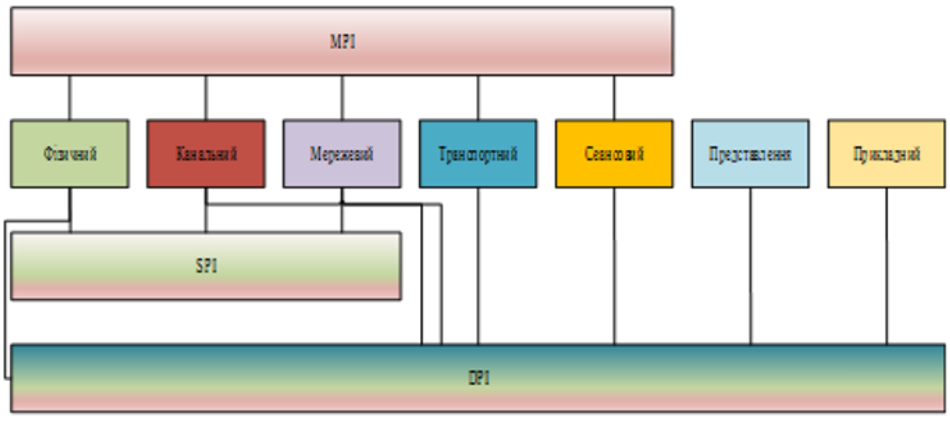
Об'єкт дослідження:трафік корпоративних мереж з пакетной комутацією.

Завдання:

- аналіз стану сучасних корпоративних мереж із пакетною комутацією щодо застосовуваних методів ідентифікації та моделей трафіку, технологій та протоколів передачі інформації;
- аналіз алгоритмів класифікації трафіку протоколів, що використовуються у корпоративних телекомунікаційних мережах;
- аналіз існуючих методів та моделей аналізу мережевих пакетів, враховучи особливості передачі данних по мережі (втрата окремих пакетів, стиснення і шифрування даних, вкладене тунелювання);
- розробка програмних засобів моніторингу корпоративної мережі з використанням досліджених моделейта методів

Переваги використання програмних засобів моніторингу КМ 3

Рівні для програмних засобів аналізу трафіка 4



Виділення і розбір заголовків протоколів в пакеті 5

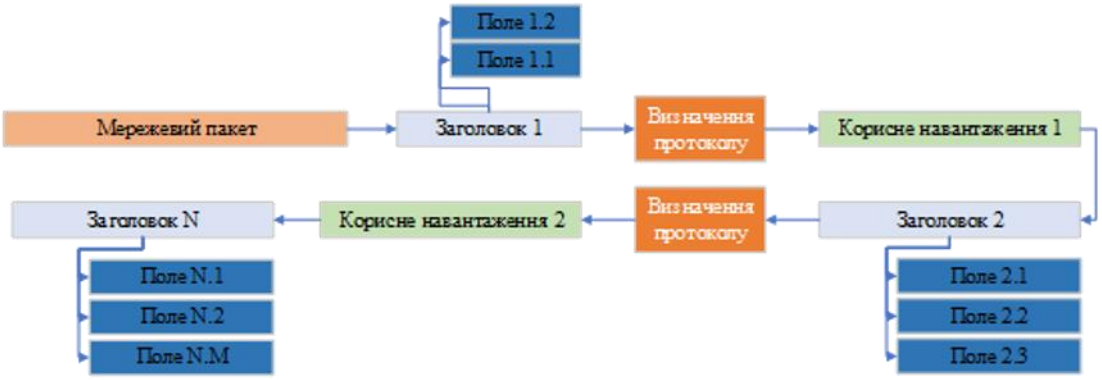
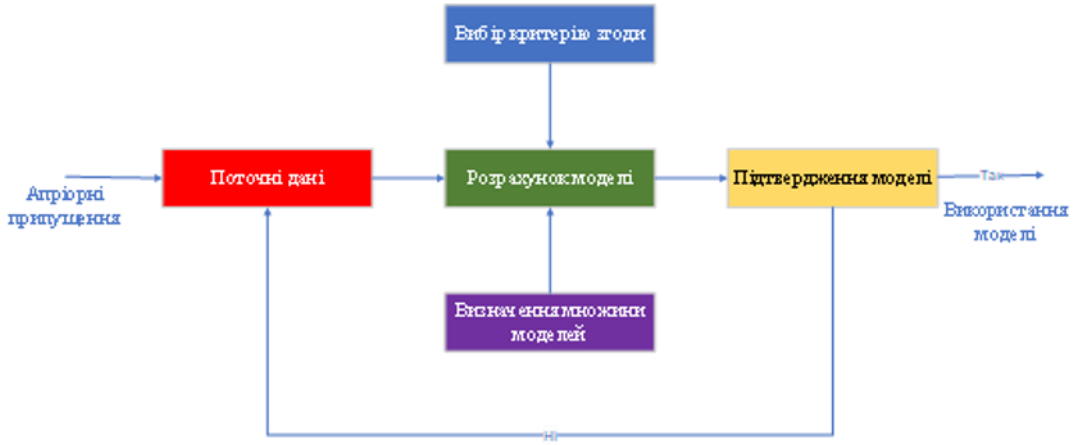


Схема ідентифікації трафіка 6



Існуючі методи ідентифікації трафіка корпоративної мережі з пакетною комутацією

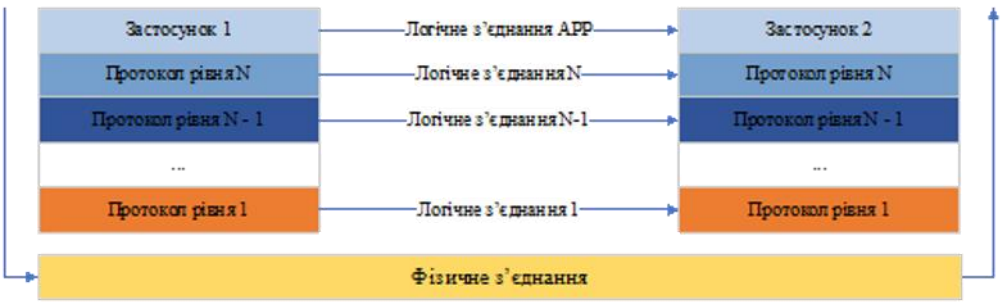
7

- Байєсовський метод.
- Методи з урахуванням фільтра Калмана
- Нейронні мережі та самонавчальні системи
- Методи, що базуються на детермінованих процесах
- Методи на основі процесів із модуляцією

Модель мережної взаємодії між двома застосунками

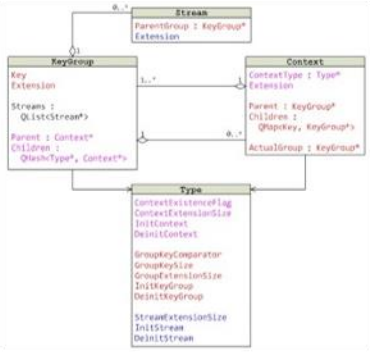
8

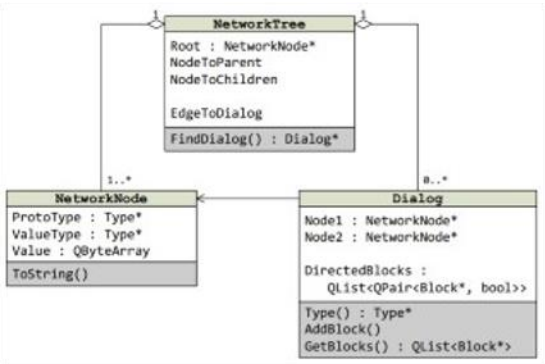
$$Packet^i = <Control^i, Payload^i> , i = 1 \dots N$$

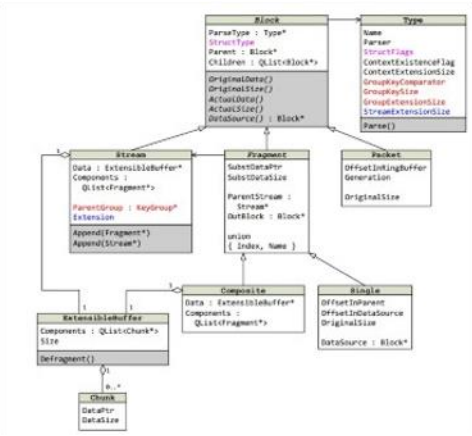


Сутності моделі

9

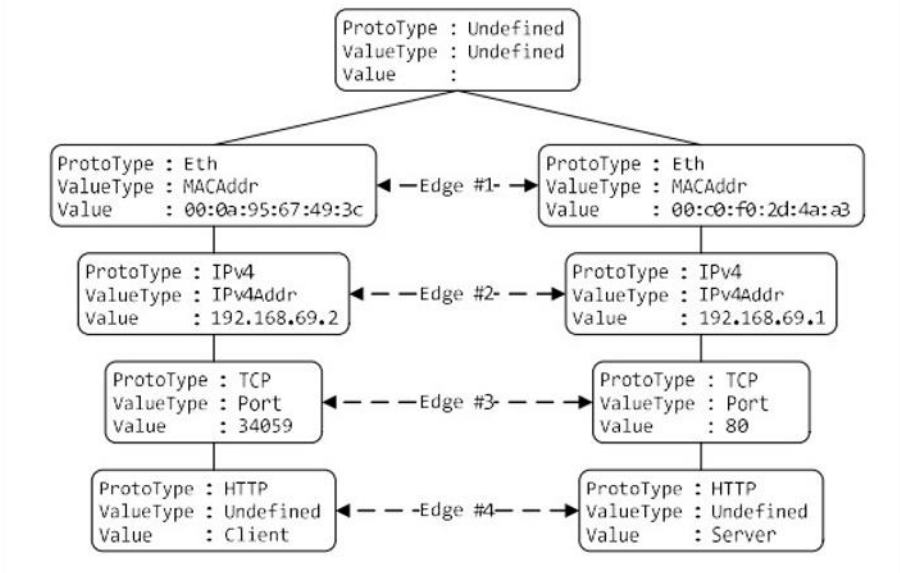






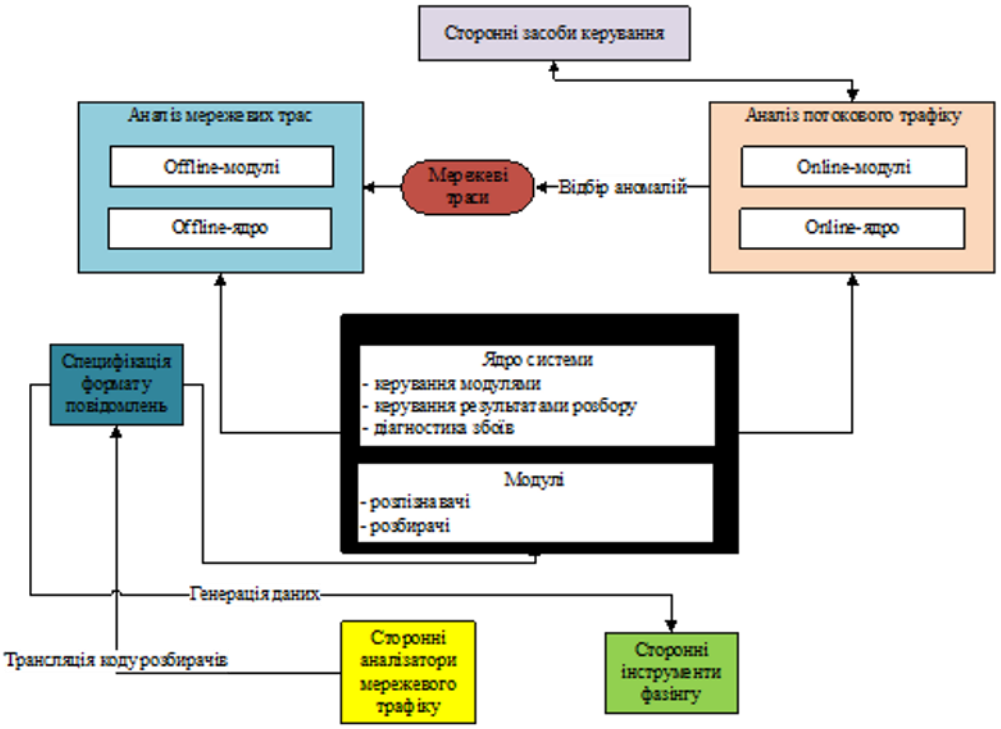
Network Tree

10



Програмні засоби моніторингу мережі для ідентифікації трафіка. Схема взаємодії програмних модулів

11



API для розробки модулів розбору та модулів побудови

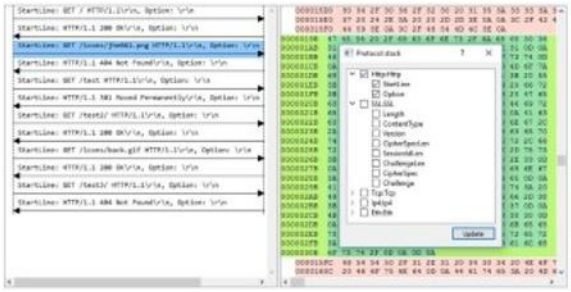
12

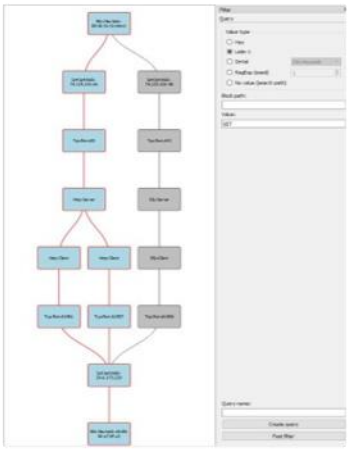
Ім'я функції	Опис
Операції над блоками	
processSingle	Створити та розібрати single-блок
processComposite	Створити та розібрати composite-блок
createStream	Створити блок-потік
completeStream	Виконати розбір блоку-потоку
streamAppend	Додати дані блока в блок-потік
Керування станом розбору	
contextExtension	Отримати дані розширення активного контексту
activateKeyGroup	Активувати в рамках поточного контекста групу
keyGroupExtension	Отримати дані розширення активної групи з ключем
setSrcDst	Активувати відправника та отримувача
Регистрація розбирачів і розпізнавачів	
regType	Зареєструвати тип
regRecognizer	Зареєструвати розпізнавач
getType	Отримати тип, який зареєстрований в іншому модулі
Журнал повідомлень	

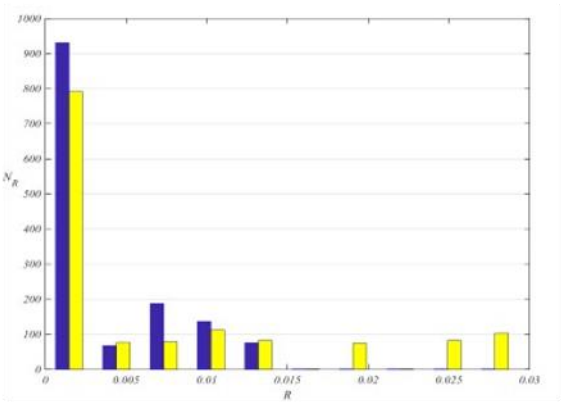
Ім'я функції	Опис
createBuffer	Створити буфер
completeBuffer	Зберегти буфер до файлу
bufferAppend	Додати дані блока в буфер у відповідності до заданого формату

Результати роботи

13







14

Висновки

В ході виконання кваліфікаційної роботи проведено аналіз алгоритмів ідентифікації, методів та технологій передачі трафіку за рахунок підвищення якості кластеризації та класифікації трафіку. Проаналізовано стан сучасних корпоративних мереж із пакетною комутацією щодо застосовуваних методів ідентифікації та моделей трафіку, технологій та протоколів передачі інформації . Також проведено аналіз алгоритмів класифікації трафіку протоколів, що використовуються у корпоративних телекомунікаційних мережах. Запропонована архітектура системи поглибленого аналізу мережевого трафіку, що дозволяє розробляти і налагоджувати модулі підтримки протоколів на попередньо збереженому трафіку і згодом використовувати ці модулі в реальному режимі часу. Розроблені та реалізовано програмні засоби для проведення моніторингу корпоративної мережі